**CLAIMS:**

1. A method for the secure storage of personal genomic information using a secure central database server residing within a sequencing service outlet comprising the steps of:

receiving and registering an individual's request to access and use said secure storage of personal genomic information system in a registration database and generating an interim unique identification code for said individual,

receiving and sequencing said individual's genomic sample to provide genomic information for said individual,

digitizing said genomic information,

applying a splitting algorithm to fragment and randomise said digitized genomic information and separating said fragmented and randomised information into at least two separate datasets,

storing at least one of said datasets in at least one portable storage device to be retained by said individual and storing the remainder of said datasets in a secure central database record,

activating said portable storage device by downloading an activation code from said secure central database server whereby said individual uses said interim unique identification code for authentication of their identity,

allocating to said individual a unique customer identifying code for customer identification and authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database,

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log-on details,

authenticating said individual's request using said customer identification code and said log-on details and comparing the input data with said registration database,

downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet

server,

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet, and

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data from said portable storage device with the data from said secure central database record and to provide said individual's genomic information in an informative format.

2. The method according to claim 1 wherein said secure central database record resides on a server which is accessed and controlled by a sequencing service outlet whereby said secure central database record is accessible on receipt of a data request from said individual using said unique customer identification code to authenticate their identity and downloading said individual portable storage device dataset into said server.

3. The method according to either of claims 1 or 2 wherein said at least two datasets include an individual's genomic information comprising nucleotide sequence information and/or annotation information generated from or relating to said individual's genetic sample plus a reconstruction key required to initiate said reconstruction algorithm residing within said sequencing service outlet secure central database server.

4. The method according to any one of claims 1 to 3 wherein said sequencing service outlet server records account transactions for each registered individual.

5. The method according to claim 4 wherein said account transactions are downloaded into hard copy format and forwarded to said individual.

6. The method according to any one of the preceding claims wherein at least two portable storage devices are forwarded to said individual whereby one portable storage device is activated and the second portable storage device is retained by said individual in a de-activated form for back-up purposes.

7. The method according to any one of the preceding claims wherein said unique identification code is in label form for tracking said individual's genomic sample and providing an interim method by which said individual can authenticate their identity.

8. The method according to any one of the preceding claims wherein said genomic sample

is taken from said individual by a pathology service provider.

9. The method according to any one of the preceding claims wherein said pathology service provider requests said unique sample identification code label from said sequencing service outlet server for attachment to said individual's genomic sample.

10. A method for the secure storage personal genomic information with a sequencing service outlet having a secure central server comprising the steps of:

registering in a registration database an individual's request for use of said secure storage of personal genomic information,

generating two copies of a unique sample identification code in label form for tracking said individual's genomic sample and providing a interim method by which said individual can authenticate their identity,

receiving said individual's genomic information having one of said unique identification labels attached,

formatting said individual's genomic information such that said genomic information is amenable to the application of a splitting algorithm,

applying a splitting algorithm to fragment and randomise said digitized genomic information and separating said fragmented and randomised information into at least two separate datasets such that, in the absence of any one dataset, the remainder of the datasets present uninformative information,

storing at least one of said datasets in at least one portable storage device and storing the remainder of said datasets in a secure central database record,

providing said portable storage device to said individual,

receiving a log-on request from said individual,

authenticating said individual using the log-on details and said interim method of authenticating said individual's identity by comparing the input data with said registration database, and approving log-on when authentication is successful,

receiving a request for portable storage device activation when said individual uses said sample identification code for re-authentication of their identity,

activating said portable storage device by downloading an activation code to said portable storage device,

allocating to said individual a unique customer identifying code for customer identification and authentication purposes where said unique customer identifying code is also allocated to said secure central database record relating to said individual and said unique customer identification code is also allocated to said individual's personal record residing in said registration database,

receiving a request from said individual to reconstruct said individual's genomic information wherein said request includes said individual's customer identification code and log-on details,

authenticating said individual's request using said customer identification code and said log-on details and comparing the input data with said registration database,

downloading said individual's personal dataset from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading a secure central database record, identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during user authentication, from said secure central database under the control of said sequencing service outlet, and

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data from said portable storage device with the data from said secure central database record and to provide said individual's genomic information in an informative format.

11. The method according to claim 10 wherein said registration database resides within the sequencing service outlet server.

12. The method according to claim 10 or 11 wherein said genomic information, having said unique sample identification code attached, is received from said individual.

13. The method according to claim 10 or 11 wherein said genomic information, having said unique sample identification code attached is received from a third party.

14. The method according to claim 13 wherein said genomic information, having said unique sample identification code attached is received from a third party a DNA sequencing provider or a pathology service provider.

15. The method according to any one of claims 10 to 14 wherein said formatting of said individual's genomic information comprises the digitization of said genomic information.

16. The method according to any one of claims 10 to 14 wherein said formatting of said individual's genomic information comprises sequencing and the digitization of said individual's genomic information.

17. The method according to any one of claims 10 to 16 wherein said at least two separate datasets include an individual's genomic information comprising nucleotide sequence information and/or annotation information generated from or relating to said individual's genomic sample plus a reconstruction key required to initiate said reconstruction algorithm residing within said sequencing service outlet secure central database server.

18. The method according to any one of claims 10 to 17 wherein said sequencing service outlet records account transactions for each registered individual.

19. The method according to any one of claims 10 to 18 wherein said account transactions are downloaded into hard copy format and forwarded to said individual.

20. The method according to any one of claims 10 to 19 wherein at least two of said portable storage devices are forwarded to said individual where one portable storage device is activated and a second portable storage device is retained by said individual in a de-activated form for back-up purposes.

21. A method for the secure storage of personal genomic information whilst enabling non-anonymous transactions with a sequencing service outlet for third party access to all or fragments of an individual's genomic information comprising the steps of:

receiving a third party request for access to personal genomic information or fragments thereof,

logging said request in a third party registration database residing within the sequencing service outlet server,

generating a unique third party customer identification code thereby providing a method by which said third party can authenticate their identity,

receiving a log-on request from said individual,

authenticating said individual using the log-on details and a customer identification code input by said individual and comparing the input data with the registration database data, and

approving log-on when authentication is successful,

receiving a third party transaction request from said individual,

recording said third party transaction request in a third party request database,

generating a unique third party transaction code for said request,

providing said third party transaction code to said individual,

receiving a third party data request from said third party which includes third party contact information, details at least the genes or genomic sequence interval and/or genomic information or portions thereof of said individual's genomic information required, to said sequencing service outlet server using said third party transaction code and said third party customer identification code for authentication of said third party,

authenticating said third party identity comparing said third party customer identification code and said third party contact information provided in said third party data request with details residing in said third party registration database, and approving third part access on successful completion of authentication,

posting of said third party data request to a data repository residing within said sequencing service outlet server for access and approval by said individual,

receiving authorisation for said third party request from said individual,

downloading said individual's personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading a secure central database record identified by said individual's customer identification code and being identical to said customer identification code entered by said individual during third party data request authorisation, from said secure central database under the control of said sequencing service outlet,

applying a reconstruction algorithm, residing within the sequencing service outlet database server to combining the data from said portable storage device with the data from said secure central database record to reproduce said individual's genomic information in an informative format,

isolating said genes or genomic sequence interval and/or genomic information or portions thereof of said genomic information according to said third party data request,

applying a splitting algorithm to fragment and randomise said digitized genomic

information and separating said fragmented and randomised information into at least two separate datasets such that, in the absence of any one dataset, the remainder of the datasets presents uninformative information,

generating a data identification code as an access label for said datasets,

storing at least one of said datasets in a third party portable storage device and storing the remainder of said datasets in a secure public dataset database record under the control of said sequencing service outlet,

providing said third party portable storage device to said third party,

activating said third party portable storage device where said third party uses said data identification code and said third party customer identification code for authentication of their identity and an activation code is downloaded to said third party portable storage device,

receiving a request from said third party to reconstruct said individual's genomic information or portions thereof where said request includes said third party customer identification code and log-on details,

authenticating said third party request using said third party identification code, third party transaction code and said log-on details and comparing the input data with said third party registration database,

downloading said individual's personal dataset from said third party portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading a secure public dataset record, identified by said third party transaction code and being identical to said third party transaction identification code entered by said third party during third party authentication, from said secure public database under the control of said sequencing service outlet, and

applying a reconstruction algorithm, residing within said sequencing service outlet database server to combine the data from said third party portable storage device with the data from said secure public database record and to provide said individual's genomic information in an informative format.

22. The method according to claim 21 wherein said third party non-anonymous transactions are available to medical laboratory, medical research, and medical diagnostic purposes and/or health care and/or medical insurance providers who register with said sequence

service outlet.

23. The method according to claim 21 or 22 wherein said data request includes said third party transaction code, said third party identification code, information relating to at least details of the genes or genomic sequence interval and/or genomic information requested by said third party and business contact details of said third party.

24. The method according to any one of claims 21 to 23 wherein said data request termination notice is posted to said third party on receipt of an unauthorised third party data request.

25. A method for the secure storage of personal genomic information whilst enabling anonymous transactions with a sequencing service outlet for third party access to whole genome sequences or fragments of an individual's genomic information comprising the steps of:

receiving, authenticating and approving if successful, a log-on request from said individual using said individual's computer log-on details and a customer identification comparing the data input with a registration database residing on a server in said sequencing service outlet,

receiving an information disclosure form request from said individual detailing at least details of the genes or genomic sequence interval and/or genomic information or portions thereof to be made available for access by an authorised third party,

downloading personal dataset information from said individual's portable storage device using a machine-readable computer interface device, to said sequencing service outlet server,

uploading of a secure central database record identified by said individual's customer identification code, from a secure central database under the control of said sequencing service outlet,

applying a reconstruction algorithm, residing within said sequencing service outlet server to combine the data from said portable storage device with the data from said secure central database record to reproduce said individual's genomic information in an informative format,

isolating and downloading said genes or genomic sequence interval and/or genomic information or portions thereof from said genomic information according to said information disclosure form request to a third party public access database record residing on a third party public access server under the control of said sequencing service outlet in a format such that said

third party public access database record is anonymous having no link to a real world identity,

receiving, authenticating and approving if successful, a log-on request from a third party to provide using a third party identification code input by said third party and comparing the input data with a third party registration database record under the control of said sequencing service outlet,

receiving a third party data request detailing at least the details of the genes or genomic sequence interval and/or genomic information or portions thereof required, to said sequencing service outlet sewer,

uploading a third party public access database record corresponding to said third party data request, and

providing said third party public access database record to said third party.

26. The method according to claim 25 wherein said anonymous third party transactions are used for medical laboratory, medical research and/or medical diagnostic purposes.

27. The method according to claim 25 or 26 wherein said information disclosure form request includes a survey to enable third parties to collect relevant phenotype information.

28. A method for the secure storage of personal genomic information using a secure central database server residing within a sequencing service outlet substantially as herein described with reference to and illustrated by the accompanying drawings.

29. A method for the secure storage of personal genomic information whilst enabling non-anonymous transactions with a sequencing service outlet for third party access to all or fragments of an individual's genomic information substantially as herein described with reference to and illustrated by the accompanying drawings.

30. A method for the secure storage of personal genomic information whilst enabling anonymous transactions with a sequencing service outlet for third party access to whole genome sequences or fragments of an individual's genomic information substantially as herein described with reference to and illustrated by the accompanying drawings.